UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/777,600	02/12/2004	Chandar Kamalanathan	DC-06380	4924

33438 7590 06/11/2009

HAMILTON & TERRILE, LLP
P.O. BOX 203518
AUSTIN, TX 78720

EXAMINER	
HAILU, TESHOME	
ART UNIT	PAPER NUMBER
2434	

NOTIFICATION DATE	DELIVERY MODE
06/11/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

tmunoz@hamiltonterrile.com

Office Action Summary	Application No.	Applicant(s)	
	10/777,600	KAMALANATHAN ET AL.	
	Examiner	Art Unit	
	TESHOME HAILU	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 March 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the Appeal Brief filed on July 23, 2008, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434

2. Claims 1-20 are pending.

3. This office action is in reply to an appeal brief filed on March 02, 2009. Claims 1-20 have been amended.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 9-17 are rejected under 35 U.S.C. 101 based on Supreme Court precedent and recent Federal Circuit decisions, a 35 U.S.C § 101 process must (1) be tied to a particular machine or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. In re

Bilski et al, 88 USPQ 2d 1385 CAFC (2008); Diamond v. Diehr, 450 U.S. 175, 184 (1981); Parker v. Flook, 437 U.S. 584, 588 n.9 (1978); Gottschalk v. Benson, 409 U.S. 63, 70 (1972); Cochrane v. Deener, 94 U.S. 780,787-88 (1876).

An example of a method claim that would not qualify as a statutory process would be a claim that recited purely mental steps. Thus, to qualify as a § 101 statutory process, the claim should positively recite the particular machine to which it is tied, for example by identifying the apparatus that accomplishes the method steps, or positively recite the subject matter that is being transformed, for example by identifying the material that is being changed to a different state.

Here, applicant's method steps are not tied to a particular machine and do not perform a transformation. Thus, the claims are non-statutory.

6. Claims 1-8 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. They are directed to functional descriptive material, which consists of a computer program per se. Since a computer program is not a process and does not fall within the statutory classes listed in 35 U.S.C. 101, the claim is believed to recite non-statuary subject matter. Appropriate correction is required.

7. Claims 18-20 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. They are directed to functional descriptive material, which consists of a computer software per se. Since a computer program is not a process and does not fall within the statutory classes listed in 35 U.S.C. 101, the claim is believed to recite non-statuary subject matter. The specification defined information handling system to include software. Since a computer program (software) is not a process and does not fall within the statutory classes listed in 35 U.S.C. 101, the claim is believed to recite non-statuary subject matter. Appropriate correction is required.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Howard et al (Howard) (US Pub. No. 2002/0069365) in view of Korn (US Pub. No. 6,880,083).

As per claim 1 Howard discloses:

Systems for secure Hypertext Markup Language (HTML) links, (page 6, paragraph 67, if the client computer is running the limited-use browser/module, the server system generates a secure HTML).

A protocol encryption tool operable to associate encrypted protocols with HTML links, (page 7, paragraph 73, the client system receives the requested content from the server system as either encrypted HTML content or secured document package).

Each protocol associated with a restricted browser function; (page 6, paragraph 67, the server system generates a secure HTML page corresponding to the requested content and sends the page to the client system).

An editor operable to publish an HTML link and associated encrypted protocol in a web page (page 1, paragraph 15, a limited-use web browser and related security system allows providers of text and images or other content to publish content on a local-area network (LAN) or wide-area network (WAN), such as world wide web (web) and the Internet). Where HTML is one way of creating a web page. “publish the content” inherently including “an editor operable to publish”.

A browser operable to display the web page and HTML link (page 1-2, paragraph 15, reads and displays any viewable web content including text, images, and streaming audio and video).

The browser having one or more restricted function, (page 6, paragraph 62, a secure document package is composed of a document manager and one or more web pages). Where the web pages can be a restricted function.

Each restricted function requiring at least selection of an HTML link (page 6, paragraph 67, the server system generates a secure HTML page corresponding to the requested content and sends the page to the client system).

A function confirmation before the browser executes the function (page 4, paragraph 42, when the user request 313 is received by the server computer 301, the server component 302 determines if a client key is associated with the request. If the key 314 in not present, the request is immediately rejected).

A protocol decryption engine interfaced with the browser, the protocol decryption engine operable to decrypt the encrypted protocol associated with the html link and authorize execution of the associated restricted browser function without the function confirmation. (Page 4, paragraph 45, when a document is secured using the common security model, the server component 302 encrypts the document prior to downloading it, and the limited user browser 312 decrypts the data for viewing only).

Howard does not explicitly disclose decrypting the encrypted protocol associated with the HTML link without the function confirmation. However, on the same field of endeavor, Korn teach this limitation as, (column 3, line 50-65, the executable commands in the script are hashed, using the same hashing function utilized at 110. The hashed commands that were encrypted and appended to the script at 120 and 130, respectively, are now decrypted at 240, using public key A, which was provided to the control at 150. The decrypted hashed commands are compared at 250 with the commands hashed at 230. If no changes in the script occurred between hashing and encrypting at 110 and 120, and hashing and decrypting at 230 and 240, the decrypted hashed commands obtained at 240 should be identical to the hashed commands obtained at 230, and the script may begin execution at 260. If, on the other hand, the commands hashed at 230 are not the same as the hashed commands decrypted at 240, the user is cautioned or warned, for example, by displaying a message in a pop up window or the like in a display screen for the client system).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Howard and include decrypting the encrypted protocol associated with the HTML link without the functional confirmation using the teaching of Korn in order to proceed with the execution of the link without the pop up window if no changes in the script occurred.

As per claim 2 Howard in view of Korn discloses:

The restricted browser function comprises a command to execute a binary. (Page 9, paragraph 96, a delivery object 701 which is the DLL binary for the document manager). Moreover, (page 4, paragraph 36, the file management system is typically stored in the mass memory 215 and cause the processor 205 to execute the various steps required by the operating system).

As per claim 3 Howard in view of Korn discloses:

The restricted browser function comprises a command to save a binary. (Page 9, paragraph 96, a delivery object 701 which is the DLL binary for the document manager). Moreover (page 4, paragraph 36, the file management system is typically stored in the mass memory 215 and cause the processor 205 to execute the various steps required by the operating system to input and output data and to store data in memory, including storing files on the mass memory 215). Where saving a file means storing a file.

As per claim 4 Howard in view of Korn discloses:

The restricted browser function comprises a command to execute a script. (Page 2, paragraph 28, any format that can be displayed via the internet, such as web graphic, common gateway interface (CGI) scripts, JAVA scripts). Where displaying a script means executing a script.

As per claim 5 Howard in view of Korn discloses:

The restricted browser function comprises a command to save a script. (Page 4, paragraph 36, the file management system is typically stored in the mass memory 215 and cause the processor 205 to

execute the various steps required by the operating system to input and output data and to store data in memory, including storing files on the mass memory 215).

As per claim 6 Howard in view of Korn discloses:

A protocol filter associated with the browser and operable to preprocess plural encrypted protocols upon retrieval of the web page by the browser. (Page 8, paragraph 86, the server security component filters web client authentication, and web server request and response events). Further Howard discloses (Page 6, paragraph 68, each document to be protected under the common security model (block 425) is marked for later encryption with the system level encryption key (SLE)).

As per claim 7 Howard in view of Korn discloses:

The protocol encryption tool comprises a private key for encryption of protocols. (Page 6, paragraph 68, each document to be protected under the common security model (block 425) is marked for later encryption with the system level encryption key (SLE)).

As per claim 8 Howard in view of Korn discloses:

Protocol decryption engine comprises a public key. (Page 6, paragraph 62, to decrypt the package, it is necessary to know where to break up the individual pages before attempting the decrypt the file and even then encryption makes the content unusable to anyone but the owner of the machine with the client registered with the unique ULE key).

As per claim 9 Howard discloses:

A method for secure HTML links, (page 6, paragraph 67, the server system generates a secure HTML).

Encrypting a protocol associated with a restricted browser function; (page 7, paragraph 73, the client system receives the requested content from the server system as either encrypted HTML content or

secured document package). Moreover, (page 6, paragraph 67, the server system generates a secure HTML page corresponding to the requested content and sends the page to the client system).

Publishing the encrypted protocol in an HTML framework to associate with an HTML link that executes the restricted browser function; (page 1, paragraph 15, a limited-use web browser and related security system allows providers of text and images or other content to publish content on a local-area network (LAN) or wide-area network (WAN), such as world wide web (web) and the Internet), where HTML is one way of creating a web page.

Displaying the HTML framework through a browser, (page 1-2, paragraph 15, reads and displays any viewable web content including text, images, and streaming audio and video).

The browser restricting execution of restricted functions by requiting a distinct confirmation before execution of the restricted function; (page 4, paragraph 42, when the user request 313 is received by the server computer 301, the server component 302 determines if a client key is associated with the request. If the key 314 in not present, the request is immediately rejected).

Decrypting the encrypted protocol at the browser; and authorizing execution of the restricted function without the distinct confirmation. (Page 4, paragraph 45, when a document is secured using the common security model, the server component 302 encrypts the document prior to downloading it, and the limited user browser 312 decrypts the data for viewing only).

Howard does not explicitly disclose decrypting the encrypted protocol without the distinct confirmation. However, on the same field of endeavor, Korn teach this limitation as, (column 3, line 50-65, the executable commands in the script are hashed, using the same hashing function utilized at 110. The hashed commands that were encrypted and appended to the script at 120 and 130, respectively, are now decrypted at 240, using public key A, which was provided to the control at 150. The decrypted hashed commands are compared at 250 with the commands hashed at 230. If no changes in the script occurred between hashing and encrypting at 110 and 120, and hashing and decrypting at 230 and 240, the decrypted hashed commands obtained at 240 should be identical to the hashed commands obtained at 230, and the script may begin execution at 260. If, on the other hand, the commands hashed at 230 are

not the same as the hashed commands decrypted at 240, the user is cautioned or warned, for example, by displaying a message in a pop up window or the like in a display screen for the client system).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Howard and include decrypting the encrypted protocol without the distinct confirmation using the teaching of Korn in order to proceed with the execution of the link without the pop up window (distinct confirmation) if no changes in the script occurred.

As per claim 10 Howard in view of Korn discloses:

Encrypting a protocol further comprises encrypting the protocol with a private key. (Page 6, paragraph 68, each document to be protected under the common security model (block 425) is marked for later encryption with the system level encryption key (SLE)).

As per claim 11 Howard in view of Korn discloses:

Decrypting the protocol further comprises decrypting the protocol with a public key. (Page 6, paragraph 62, to decrypt the package, it is necessary to know where to break up the individual pages before attempting the decrypt the file and even then encryption makes the content unusable to anyone but the owner of the machine with the client registered with the unique ULE key).

As per claim 12 Howard in view of Korn discloses:

Authorizing execution of restricted function further comprises authorizing execution of a binary by the browser. (Page 9, paragraph 96, a delivery object 701 which is the DLL binary for the document manager"). Moreover (page 4, paragraph 36, the file management system is typically stored in the mass memory 215 and cause the processor 205 to execute the various steps required by the operating system).

As per claim 13 Howard in view of Korn discloses:

Authorizing execution of the restricted function further comprises authorizing saving of a binary by the browser. (Page 9, paragraph 96, a delivery object 701 which is the DLL binary for the document manager"). Moreover (page 4, paragraph 36, the file management system is typically stored in the mass memory 215 and cause the processor 205 to execute the various steps required by the operating system to input and output data and to store data in memory, including storing files on the mass memory 215). Where saving a file means storing a file.

As per claim 14 Howard in view of Korn discloses:

Authorizing execution of the restricted function further comprises authorizing execution of a script by the browser. (Page 2, paragraph 28, any format that can be displayed via the internet, such as web graphic, common gateway interface (CGI) scripts, JAVA scripts). Where displaying a script means executing a script.

As per claim 15 Howard in view of Korn discloses:

Authorizing execution of the restricted function further comprises authorizing saving of a script by the browser. (Page 4, paragraph 36, the file management system is typically stored in the mass memory 215 and cause the processor 205 to execute the various steps required by the operating system to input and output data and to store data in memory, including storing files on the mass memory 215).

As per claim 16 Howard in view of Korn discloses:

Preprocessing of plural encrypted protocols substantially upon loading of the HTML framework to the browser. (Page 6, paragraph 68, each document to be protected under the common security model (block 425) is marked for later encryption with the system level encryption key (SLE)).

As per claim 17 Howard in view of Korn discloses:

The distinct confirmation comprises a window displayed upon user selection of an HTML link associated with a restricted function, the window requiring at least one addition input by the user before

execution of the restricted function. (Page 1-2, paragraph 15, reads and displays any viewable web content including text, images, and streaming audio and video).

As per claim 18 Howard discloses:

An information handling system comprising: (page 1, paragraph 11, secure information distribution system).

A browser operable to retrieve and display a HTML link associated with a restricted function, (page 7, paragraph 73, the client system receives the requested content from the server system as either encrypted HTML content or secured document package).

The browser requiring a distinct confirmation of a selection of the HTML link before execution of the restricted function; (page 4, paragraph 42, when the user request 313 is received by the server computer 301, the server component 302 determines if a client key is associated with the request. If the key 314 in not present, the request is immediately rejected).

An encrypted protocol associated with the HTML link; (page 6, paragraph 60, the HTML source code is encrypted by the server digital processing system using a system level encryption (SLE) key).

A protocol decryption engine interfaced with the browser and operable to override the distinct confirmation requirement upon decryption and validation of the encrypted protocol. (Page 4, paragraph 45, when a document is secured using the common security model, the server component 302 encrypts the document prior to downloading it, and the limited user browser 312 decrypts the data for viewing only). Further Howard discloses, (page 4, paragraph 42, when the user request 313 is received by the server computer 301, the server component 302 determines if a client key is associated with the request. If the key 314 in not present, the request is immediately rejected).

Howard does not explicitly disclose overriding the distinct confirmation requirement upon decrypting the encrypted protocol. However, on the same field of endeavor, Korn teach this limitation as, (column 3, line 50-65, the executable commands in the script are hashed, using the same hashing function utilized at 110. The hashed commands that were encrypted and appended to the script at 120 and 130, respectively, are now decrypted at 240, using public key A, which was provided to the control at

150. The decrypted hashed commands are compared at 250 with the commands hashed at 230. If no changes in the script occurred between hashing and encrypting at 110 and 120, and hashing and decrypting at 230 and 240, the decrypted hashed commands obtained at 240 should be identical to the hashed commands obtained at 230, and the script may begin execution at 260. If, on the other hand, the commands hashed at 230 are not the same as the hashed commands decrypted at 240, the user is cautioned or warned, for example, by displaying a message in a pop up window or the like in a display screen for the client system).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Howard and include overriding the distinct confirmation requirement upon decrypting using the teaching of Korn in order to proceed with the execution of the link without the pop up window (overriding the distinct confirmation) if no changes in the script occurred.

As per claim 19 Howard in view of Korn discloses:

Browser is further operable to retrieve a web page having plural encrypted protocols, (page 6, paragraph 62, a secure document package is composed of a document manager and one or more web pages, each of which is encrypted with the ULE).

The information handling system further comprising, (page 1, paragraph 11, secure information distribution system)

A protocol filter interfaced with the browser and operable to identify the plural encrypted protocols for decrypting by the protocol decryption engine. (Page 8, paragraph 86, the server security component filters web client authentication, and web server request and response events). Further Howard discloses (Page 6, paragraph 68, each document to be protected under the common security model (block 425) is marked for later encryption with the system level encryption key (SLE)).

As per claim 20 Howard in view of Korn discloses:

A protocol database interfaced with the protocol decryption engine and having a table of protocols and associated restricted functions, (Page 6, paragraph 62, to decrypt the package, it is necessary to

know where to break up the individual pages before attempting the decrypt the file and even then encryption makes the content unusable to anyone but the owner of the machine with the client registered with the unique ULE key).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TESHOME HAILU whose telephone number is (571)270-3159. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m. EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Teshome Hailu/

Examiner, Art Unit 2434

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434